

Andrew G. Gunem (SBN 354042)
agunem@straussborrelli.com
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue
Suite 1610
Chicago IL, 60611

Attorneys for Plaintiff and Proposed Class

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

MICHAEL MCCARTHY, on behalf of
himself and all others similarly situated,

Plaintiff,

v.

LAGUNITAS BREWING COMPANY,

Defendant.

Case No. 3:24-cv-02641

CLASS ACTION COMPLAINT

- 1. Negligence**
- 2. Negligence *per se***
- 3. Breach of Implied Contract**
- 4. Unjust Enrichment**
- 5. Invasion of Privacy**
- 6. Breach of Fiduciary Duty**
- 7. Violation of the California Unfair Competition Law**
- 8. Violation of the California Consumer Privacy Act**

DEMAND FOR JURY TRIAL

Plaintiff, Michael McCarthy (“Plaintiff”), on behalf of himself and all others similarly situated, states as follows for his class action complaint against Defendant, Lagunitas Brewing Company (“Lagunitas” or “Defendant”):

INTRODUCTION

1. On information and belief, the Data Breach occurred on March 12, 2024. Following an internal investigation, Defendant learned cybercriminals had gained unauthorized access to employees’ personally identifiable information (“PII”).

1 2. However, due to intentionally obfuscating language, Lagunitas has refused to
2 identify what specific PII has been exposed in the Data Breach, admitting only that it includes
3 information in current and former employees' I-9. Upon information and belief, I-9's includes date
4 of birth, name, passport number, driver's license number, and Social Security number.

5 3. On or about April 26, 2024—over a month after the Data Breach occurred—
6 Lagunitas finally began notifying Class Members about the Data Breach ("Breach Notice"). A
7 sample Breach Notice to Maine residents is attached as Exhibit A. Plaintiff's breach notice is
8 attached as Exhibit B.

9 4. Upon information and belief, cybercriminals were able to breach Defendant's
10 systems because Defendant failed to adequately train its employees on cybersecurity, failed to
11 adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII
12 of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's
13 PII—rendering it an easy target for cybercriminals.

14 5. Defendant's Breach Notice obfuscated the nature of the breach and the threat it
15 posted—refusing to tell its employees how many people were impacted, how the breach happened,
16 or why it took the Defendant over a month to finally begin notifying some victims that
17 cybercriminals had gained access to their highly private information.

18 6. Defendant's failure to timely report the Data Breach made the victims vulnerable
19 to identity theft without any warnings to monitor their financial accounts or credit reports to
20 prevent unauthorized use of their PII.

21 7. Defendant knew or should have known that each victim of the Data Breach
22 deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of
23 PII misuse.

24 8. In failing to adequately protect its employees' information, adequately notify them
25 about the breach, and obfuscating the nature of the breach, Defendant violated state law and
26 harmed an unknown number of its current and former employees.

9. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiff is a former Lagunitas employee and Data Breach victim.

11. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and insecure.

PARTIES

12. Plaintiff, Michael McCarthy, is a natural person and citizen of Illinois, residing in Chicago, Illinois, where he intends to remain.

13. Defendant, Lagunitas, is incorporated in California, with its principal place of business at 1280 North McDowell Boulevard Petaluma, California 94954.

JURISDICTION & VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. There are over 100 putative Class Members.

15. This Court has personal jurisdiction over Defendant because it is headquartered in Georgia, and regularly conducts business in California. Plaintiff and Defendant are from different states.

16. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS***Lagunitas***

17. Lagunitas, an American beer company headquartered in Petaluma, California, touts its product availability throughout at least 20 countries.”¹ It further boasts over \$102 million in annual revenue.²

18. On information and belief, Lagunitas accumulates highly private PII of its employees.

19. In collecting and maintaining its employees’ PII, Defendant agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

20. Indeed, Lagunitas boasts in its privacy policy that it intends to “protect against the loss, misuse, or alteration of information” it collects and “employ reasonable security measures to protect the security of [that] information[.]”

SECURITY

It is our intent to protect against the loss, misuse, or alteration of information that we have collected from you. We employ reasonable security measures to protect the security of the information you submit to us. We limit the information we provide to outside companies with whom we contract to only what they need to carry out their responsibilities. When you make a purchase, request product information or create an account on our website, your transactional information is transmitted in a safe, encrypted format. We maintain the data you provide, along with a record of your purchases, in a secure database.

21. Lagunitas understood the need to protect its current and former employees’ PII and prioritize its data security.

22. Despite recognizing its duty to do so, on information and belief, Lagunitas has not implemented reasonably cybersecurity safeguards or policies to protect employee PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result,

¹ Lagunitas Brewing Company, About Us, <https://www.linkedin.com/company/lagunitas-brewing-co-/about/> (last visited May 2, 2024).

² Lagunitas Brewing Company, RocketReach, https://rocketreach.co/lagunitas-brewing-company-profile_b5dec260f42e4f2c (last visited May 2, 2024).

Lagunitas leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' PII.

Lagunitas Fails to Safeguard Employees' PII

23. Plaintiff is a former employee of Lagunitas.

24. As a condition of employment with Lagunitas, Plaintiff provided Defendant with his PII, including information related to I-9, such as date of birth, name, passport number, driver's license number, and Social Security number. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

25. On information and belief, Lagunitas collects and maintains employees' unencrypted PII in its computer systems.

26. In collecting and maintaining PII, Defendant implicitly agreed that it will safeguard the data using reasonable means according to its internal policy, state and federal law.

27. According to the Breach Notice, Lagunitas claims that "[o]n or about March 12, 2024, [it] received internal reports of suspicious activity[.]" Lagunitas further admits that an internal investigation revealed that the Data breach "resulted in the unauthorized acquisition of personal information of some employees and their beneficiaries." Exs. A and B.

28. In other words, the Data Breach investigation revealed Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its employees' highly private information.

29. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

30. Upon information and belief, the notorious Black Basta ransomware gang was responsible for the cyberattack. Known as one of the most notorious and active ransomware actors infamous for its double extortion method³, that raked in at least \$100 million in ransom payment

³ Black Basta ransomware, Threat Profile, chrome-

through just 90 victims, Black Basta has perpetrated multiple high-profile breaches in the last year alone.⁴ Lagunitas knew or should have known of the tactics that groups like Black Basta employ.

31. With the Sensitive Information secured and stolen by Black Basta, the hackers then purportedly issued a ransom demand to Lagunitas. However, Lagunitas has provided no public information on the ransom demand or payment.



2024-03-27	lagunitas.com	The Lagunitas Brewing Company began on a kitchen stove in Northern California in 1993 and has been crafting hop-forward beers ever since. Welcoming the open-minded with open taps and simple truths: Beer Speaks (for itself), Life Is Uncertain (don't sip), and It's Good To Have Friends. To quote our BrewMonster, "Lagunitas is made up of all kinds and creeds; punk rockers, misfits, ivy leaguers, weirdos, Waldos, Sparkle Ponies, Musicians, and everything in between ... Just a pack of stray dogs that found—despite our vast and wild differences—that the love and respect for the freedom to be different is what brought us together and made it all work." Whether we're supporting local communities by turning beer into money for the cause, or simply fueling stories and songs with IPA and other creations—we always have a spot for you at our bar. Come as you are. And bring your dog, too. Here's how it all really happened, or at least how we remember it. Heck... we don't remember a lot, so this is at least how we thought it might have gone or something...SITE: www.lagunitas.comADDRESS: 1280 N. McDowell Boulevard Petaluma, Calif. 94954 USAALL DATA SIZE: ~700gb 1. All data company 2. Users personal data & etc...
------------	---------------	---

32. On information or belief, Black Basta released all stolen information onto the dark web for access, sale, and download following the deadline of the ransom demand to Defendant.

33. On or about April 26, 2024—over a month after the Data Breach occurred—Lagunitas finally began notifying some Class Members about the Data Breach.

34. Despite its duties to safeguard PII, Defendant, a self-proclaimed leader in its industry, did not in fact follow industry standard practices in securing employees' PII, as evidenced by the Data Breach.

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf (last accessed May 2, 2024).

⁴ Black Basta ransomware, Bleeping Computer, <https://www.bleepingcomputer.com/news/security/black-basta-ransomware-made-over-100-million-from-extortion/> (last accessed May 2, 2024).

1 35. In response to the Data Breach, Lagunitas contends that it is “implement(ing)
2 additional security measures.” Ex. A. Although Defendant fails to expand on what these
3 “additional security measures” are, such measures should have been in place before the Data
4 Breach.

5 36. Through its Breach Notice, Defendant recognized the actual imminent harm and
6 injury that flowed from the Data Breach, so it encouraged breach victims to be “remain vigilant in
7 regularly reviewing your account statements and monitoring your accounts for suspicious
8 activity.” Ex. A.

9 37. Through the Data Breach, Defendant recognized its duty to implement reasonable
10 cybersecurity safeguards or policies to protect employees’ PII, insisting that, despite the Data
11 Breach demonstrating otherwise, “the privacy and security of your information are important to
12 Lagunitas.” Ex’s. A and B.

13 38. Defendant further recognized through its Breach Notice, its obfuscating language
14 and failure to provide adequate information regarding the Data Breach in the Breach notice,
15 including obfuscating what PII of its victims were involved, advising victims to “contact the
16 dedicated toll-free customer service line regarding any questions or to request assistance.” Ex’s.
17 A and B.

18 39. On information and belief, Lagunitas has offered several months of complimentary
19 credit monitoring services to victims, which does not adequately address the lifelong harm that
20 victims will face following the Data Breach. Indeed, the breach involves PII that cannot be
21 changed, such as Social Security numbers. Further, due to Defendant’s failure to provide adequate
22 notice, some victims, including Plaintiff, are unable to access the credit monitoring offered by
23 Defendant.

24 40. Even with several months of credit monitoring services, the risk of identity theft
25 and unauthorized use of Plaintiff’s and Class Members’ PII is still substantially high. The
26 fraudulent activity resulting from the Data Breach may not come to light for years.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

42. On information and belief, Lagunitas failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

43. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

44. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.⁵

45. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Lagunitas knew or should have known that its electronic records would be targeted by cybercriminals.

46. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

47. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its

⁵ Data breaches break record in 2021, CNET (Jan. 24, 2022), <https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/> (last accessed September 4, 2023).

own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

48. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

49. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."⁶

50. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."⁷

51. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."⁸

⁶ High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at <https://www.ic3.gov/Media/Y2019/PSA191002> (last accessed September 4, 2023).

⁷ Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last accessed September 4, 2023).

⁸ Ransomware Guide, U.S. CISA, <https://www.cisa.gov/stopransomware/ransomware-guide> (last accessed September 4, 2023).

52. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

53. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of thousands of its current and former employees in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

54. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

55. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its employees' Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Plaintiff's Experience and Injuries

56. Plaintiff Michael McCarthy is a former employee of Defendant and a data breach victim.

57. As a condition of employment, Lagunitas required Mr. McCarthy to provide his PII, including at least his name and Social Security Number in order to receive employment.

58. Mr. McCarthy provided his PII to Lagunitas and trusted that the company would use reasonable measures to protect it according to its internal policy, as well as state and federal law.

59. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about the Breach. Indeed, Plaintiff and his counsel were forced to contact Defendant to confirm that Plaintiff's PII had been impacted by the Breach.

60. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

61. Plaintiff suffered actual injury from the exposure of his PII—which violates his rights to privacy.

62. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

63. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring Mr. McCarthy credit information.

64. Plaintiff has already spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

65. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach.

66. Indeed, following the Data Breach, Plaintiff has experienced an increase in phishing calls, many of which claim to be IRS, tax, and UPS package delivery related, further suggesting that his PII is now in the hands of cybercriminals.

67. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.⁹ On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

68. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

69. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

70. As a result of Lagunitas failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the class have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise and continuing publication of their PII;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;

⁹ What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-do-hackers-do-with-stolen-information> (last visited January 9, 2024).

1 g. Unauthorized use of stolen PII; and

2 h. The continued risk to their PII, which remains in the possession of Defendant
3 and is subject to further breaches so long as Defendant fails to undertake the
4 appropriate measures to protect the PII in its possession.

5 71. Stolen PII is one of the most valuable commodities on the criminal information
6 black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to
7 \$1,000.00 depending on the type of information obtained.

8 72. The value of Plaintiff's and the proposed Class's PII on the black market is
9 considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen
10 private information openly and directly on various "dark web" internet websites, making the
11 information publicly available, for a substantial fee of course.

12 73. Social Security numbers are particularly attractive targets for hackers because they
13 can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover,
14 Social Security numbers are difficult to replace, as victims are unable to obtain a new number until
15 the damage is done.

16 74. It can take victims years to spot identity or PII theft, giving criminals plenty of time
17 to use that information for cash.

18 75. One such example of criminals using PII for profit is the development of "Fullz"
19 packages.

20 76. Cyber-criminals can cross-reference two sources of PII to marry unregulated data
21 available elsewhere to criminally stolen data with an astonishingly complete scope and degree of
22 accuracy in order to assemble complete dossiers on individuals. These dossiers are known as
23 "Fullz" packages.

24 77. The development of "Fullz" packages means that stolen PII from the Data Breach
25 can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email
26 addresses, and other unregulated sources and identifiers. In other words, even if certain
27 information such as emails, phone numbers, or credit card numbers may not be included in the PII
28

1 stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and
2 sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam
3 telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is
4 reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members
5 of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data
6 Breach.

7 78. Defendant disclosed the PII of Plaintiff and members of the proposed Class for
8 criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed,
9 and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful
10 business practices and tactics, including online account hacking, unauthorized use of financial
11 accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all
12 using the stolen PII.

13 79. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach
14 exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take
15 appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused
16 by the Data Breach.

17 ***Defendant failed to adhere to FTC guidelines.***

18 80. According to the Federal Trade Commission ("FTC"), the need for data security
19 should be factored into all business decision-making. To that end, the FTC has issued numerous
20 guidelines identifying best data security practices that businesses, such as Defendant, should
21 employ to protect against the unlawful exposure of PII.

22 81. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide
23 for Business, which established guidelines for fundamental data security principles and practices
24 for business. The guidelines explain that businesses should:

- 25 a. protect the personal customer information that they keep;
- 26 b. properly dispose of personal information that is no longer needed;
- 27 c. encrypt information stored on computer networks;

1 d. understand their network's vulnerabilities; and

2 e. implement policies to correct security problems.

3 82. The guidelines also recommend that businesses watch for large amounts of data
4 being transmitted from the system and have a response plan ready in the event of a breach.

5 83. The FTC recommends that companies not maintain information longer than is
6 needed for authorization of a transaction; limit access to sensitive data; require complex passwords
7 to be used on networks; use industry-tested methods for security; monitor for suspicious activity
8 on the network; and verify that third-party service providers have implemented reasonable security
9 measures.

10 84. The FTC has brought enforcement actions against businesses for failing to
11 adequately and reasonably protect customer data, treating the failure to employ reasonable and
12 appropriate measures to protect against unauthorized access to confidential consumer data as an
13 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15
14 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take
15 to meet their data security obligations.

16 85. Defendant's failure to employ reasonable and appropriate measures to protect
17 against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by
18 Section 5 of the FTCA, 15 U.S.C. § 45.

19 ***Defendant Failed to Follow Industry Standards***

20 86. Several best practices have been identified that—at a minimum—should be
21 implemented by businesses like Defendant. These industry standards include: educating all
22 employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-
23 malware software; encryption (making data unreadable without a key); multi-factor authentication;
24 backup data; and limiting which employees can access sensitive data.

25 87. Other industry standard best practices include: installing appropriate malware
26 detection software; monitoring and limiting the network ports; protecting web browsers and email
27 management systems; setting up network systems such as firewalls, switches, and routers;

1 monitoring and protection of physical security systems; protection against any possible
2 communication system; and training staff regarding critical points.

3 88. Defendant failed to meet the minimum standards of any of the following
4 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation
5 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,
6 PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for
7 Internet Security's Critical Security Controls (CIS CSC), which are all established standards in
8 reasonable cybersecurity readiness.

9 89. These frameworks are applicable and accepted industry standards. And by failing
10 to comply with these accepted standards, Defendant opened the door to the criminals—thereby
11 causing the Data Breach.

12 CLASS ACTION ALLEGATIONS

13 90. Plaintiff is suing on behalf of himself and the proposed Class ("Class"), defined as
14 follows:

15 **All individuals residing in the United States whose PII was**
16 **compromised in Defendant's Data Breach, including all those**
who received notice of the breach.

17 91. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries,
18 any entity in which Defendant has a controlling interest, any Defendant officer or director, any
19 successor or assign, and any Judge who adjudicates this case, including their staff and immediate
20 family.

21 92. Plaintiff reserves the right to amend the class definition.

22 93. This action satisfies the numerosity, commonality, typicality, and adequacy
23 requirements under Fed. R. Civ. P. 23.

24 a. **Numerosity**. Plaintiff's claim is representative of the proposed Class,
25 consisting of almost three thousand individuals, far too many to join in a single action;
26
27
28

1 b. **Ascertainability**. Class members are readily identifiable from information
2 in Defendant's possession, custody, and control;

3 c. **Typicality**. Plaintiff's claim is typical of Class member's claims as each
4 arises from the same Data Breach, the same alleged violations by Defendant, and the same
5 unreasonable manner of notifying individuals about the Data Breach.

6 d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's
7 interests. His interest does not conflict with Class members' interests, and Plaintiff has retained
8 counsel experienced in complex class action litigation and data privacy to prosecute this action on
9 the Class's behalf, including as lead counsel.

10 e. **Commonality**. Plaintiff's and the Class's claims raise predominantly
11 common fact and legal questions that a class wide proceeding can answer for all Class members.
12 Indeed, it will be necessary to answer the following questions:

- 13 i. Whether Defendant had a duty to use reasonable care in safeguarding
14 Plaintiff's and the Class's PII;
 - 15 ii. Whether Defendant failed to implement and maintain reasonable
16 security procedures and practices appropriate to the nature and scope of
17 the information compromised in the Data Breach;
 - 18 iii. Whether Defendant was negligent in maintaining, protecting, and
19 securing PII;
 - 20 iv. Whether Defendant breached contract promises to safeguard Plaintiff's
21 and the Class's PII;
 - 22 v. Whether Defendant took reasonable measures to determine the extent
23 of the Data Breach after discovering it;
 - 24 vi. Whether Defendant's Breach Notice was reasonable;
 - 25 vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;
 - 26 viii. What the proper damages measure is; and
- 27
28

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

f. **Appropriateness.** The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case. Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

g. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

94. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

95. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

96. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

97. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

98. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff's and Class Members' PII.

1 99. Defendant owed—to Plaintiff and Class Members—at least the following duties
2 to:

- 3 a. exercise reasonable care in handling and using the PII in its care and custody;
- 4 b. implement industry-standard security procedures sufficient to reasonably protect
5 the information from a data breach, theft, and unauthorized;
- 6 c. promptly detect attempts at unauthorized access;
- 7 d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to
8 the security of their PII.

9 100. Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class
10 Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and
11 necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be
12 vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the
13 harm caused by the Data Breach.

14 101. Defendant also had a duty to exercise appropriate clearinghouse practices to remove
15 PII it was no longer required to retain under applicable regulations.

16 102. Defendant knew or reasonably should have known that the failure to exercise due
17 care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an
18 unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal
19 acts of a third party.

20 103. Defendant's duty to use reasonable security measures arose because of the special
21 relationship that existed between Defendant and Plaintiff and the Class. That special relationship
22 arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary
23 part of employment from Defendant.

24 104. The risk that unauthorized persons would attempt to gain access to the PII and
25 misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that
26 unauthorized individuals would attempt to access Defendant's databases containing the PII —
27 whether by malware or otherwise.

1 105. PII is highly valuable, and Defendant knew, or should have known, the risk in
2 obtaining, using, handling, emailing, and storing the PII of Plaintiff's and Class Members' and the
3 importance of exercising reasonable care in handling it.

4 106. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the
5 Class in deviation of standard industry rules, regulations, and practices at the time of the Data
6 Breach.

7 107. Defendant breached these duties as evidenced by the Data Breach.

8 108. Defendant acted with wanton and reckless disregard for the security and
9 confidentiality of Plaintiff's and Class Members' PII by:

- 10 a. disclosing and providing access to this information to third parties and
11 b. failing to properly supervise both the way the PII was stored, used, and exchanged,
12 and those in its employ who were responsible for making that happen.

13 109. Defendant breached its duties by failing to exercise reasonable care in supervising
14 its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and
15 Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class
16 Members' injury.

17 110. Defendant further breached its duties by failing to provide reasonably timely notice
18 of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and
19 exacerbated the harm from the Data Breach and Plaintiff's and Class Members' injuries-in-fact.

20 111. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost
21 and disclosed to unauthorized third persons because of the Data Breach.

22 112. As a direct and traceable result of Defendant's negligence and/or negligent
23 supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary
24 damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional
25 distress.

26 113. Defendant's breach of its common-law duties to exercise reasonable care and its
27 failures and negligence actually and proximately caused Plaintiff and Class Members actual,
28

1 tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by
 2 criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and
 3 lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted
 4 from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing,
 5 imminent, immediate, and which they continue to face.

6 **SECOND CLAIM FOR RELIEF**
 7 **Negligence *per se***
 8 **(On Behalf of Plaintiff and the Class)**

9 114. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

10 115. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate
 11 computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

12 116. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce,"
 13 including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as
 14 Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC
 15 publications and orders promulgated pursuant to the FTC Act also form part of the basis of
 16 Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

17 117. Defendant breached its respective duties to Plaintiff and Class Members under the
 18 FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security
 19 practices to safeguard PII.

20 118. Defendant violated its duty under Section 5 of the FTC Act by failing to use
 21 reasonable measures to protect PII and not complying with applicable industry standards as
 22 described in detail herein. Defendant's conduct was particularly unreasonable given the nature and
 23 amount of PII Defendant had collected and stored and the foreseeable consequences of a data
 24 breach, including, specifically, the immense damages that would result to individuals in the event
 25 of a breach, which ultimately came to pass.

26 119. The harm that has occurred is the type of harm the FTC Act is intended to guard
 27 against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,
 28

1 because of their failure to employ reasonable data security measures and avoid unfair and deceptive
2 practices, caused the same harm as that suffered by Plaintiff and members of the Class.

3 120. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and
4 Class Members would not have been injured.

5 121. The injury and harm suffered by Plaintiff and Class Members was the reasonably
6 foreseeable result of Defendant's breach of their duties. Defendant knew or should have known
7 that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members
8 of the Class to suffer the foreseeable harms associated with the exposure of their PII.

9 122. Defendant's violations and its failure to comply with applicable laws and
10 regulations constitutes negligence *per se*.

11 123. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and
12 Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*)

13 **THIRD CLAIM FOR RELIEF**
14 **Breach of Implied Contract**
15 **(On Behalf of Plaintiff and the Class)**

16 124. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

17 125. Defendant offered to employ Plaintiff and members of the Class if, as a condition
18 of that employment, Plaintiff and members of the Class provided Defendant with their PII.

19 126. In turn, Defendant agreed it would not disclose the PII it collects to unauthorized
20 persons. Defendant also promised to safeguard employee PII.

21 127. Plaintiff and the members of the Class accepted Defendant's offer by providing PII
22 to Defendant in exchange for employment with Defendant.

23 128. Implicit in the parties' agreement was that Defendant would provide Plaintiff and
24 members of the Class with prompt and adequate notice of all unauthorized access and/or theft of
25 their PII.

26 129. Plaintiff and the members of the Class would not have entrusted their PII to
27 Defendant in the absence of such an agreement with Defendant.

1 130. Defendant materially breached the contracts it had entered with Plaintiff and
2 members of the Class by failing to safeguard such information and failing to notify them promptly
3 of the intrusion into its computer systems that compromised such information. Defendant also
4 breached the implied contracts with Plaintiff and members of the Class by:

- 5 a. Failing to properly safeguard and protect Plaintiff's and members of the Class's
6 PII;
- 7 b. Failing to comply with industry standards as well as legal obligations that are
8 necessarily incorporated into the parties' agreement; and
- 9 c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant
10 created, received, maintained, and transmitted.

11 131. The damages sustained by Plaintiff and members of the Class as described above
12 were the direct and proximate result of Defendant's material breaches of its agreement(s).

13 132. Plaintiff and members of the Class have performed under the relevant agreements,
14 or such performance was waived by the conduct of Defendant.

15 133. The covenant of good faith and fair dealing is an element of every contract. All
16 such contracts impose upon each party a duty of good faith and fair dealing. The parties must act
17 with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in
18 connection with executing contracts and discharging performance and other duties according to
19 their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the
20 parties to a contract are mutually obligated to comply with the substance of their contract in
21 addition to its form.

22 134. Subterfuge and evasion violate the obligation of good faith in performance even
23 when an actor believes their conduct to be justified. Bad faith may be overt or may consist of
24 inaction, and fair dealing may require more than honesty.

25 135. Defendant failed to advise Plaintiff and members of the Class of the Data Breach
26 promptly and sufficiently.

27 136. In these and other ways, Defendant violated its duty of good faith and fair dealing.
28

138. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

139. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

140. This claim is plead in the alternative to the breach of implied contractual duty claim.

141. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment. Defendant also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate their employment.

142. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

143. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

144. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

145. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

146. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

147. Defendant owed a duty to its employees, including Plaintiff and the Class, to keep this information confidential.

148. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

149. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of their employment, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

150. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

151. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

152. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

153. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

1 161. Because of the highly sensitive nature of the PII, Plaintiff and Class members would
2 not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known
3 the reality of Defendant's inadequate data security practices.

4 162. Defendant breached its fiduciary duties to Plaintiff and Class members by failing
5 to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

6 163. Defendant also breached its fiduciary duties to Plaintiff and Class members by
7 failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and
8 practicable period.

9 164. As a direct and proximate result of Defendant's breach of its fiduciary duties,
10 Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as
11 detailed *supra*).

12 **SIXTH CLAIM FOR RELIEF**
13 **Violation of California's Unfair Competition Law (UCL)**
14 **Cal. Bus. & Prof. Code § 17200, et seq.**
 (On Behalf of the Plaintiff and the Class)

15 165. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

16 166. Defendant engaged in unlawful and unfair business practices in violation of Cal.
17 Bus. & Prof. Code § 17200, et seq. which prohibits unlawful, unfair, or fraudulent business acts
18 or practices ("UCL").

19 167. Defendant's conduct is unlawful because it violates the California Consumer
20 Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security
21 laws.

22 168. Defendant stored the PII of Plaintiff and the Class in its computer systems and knew
23 or should have known it did not employ reasonable, industry standard, and appropriate security
24 measures that complied with applicable regulations and that would have kept Plaintiff's and the
25 Class's PII secure to prevent the loss or misuse of that PII.
26
27
28

1 169. Defendant failed to disclose to Plaintiff and the Class that their PII was not secure.
2 However, Plaintiff and the Class were entitled to assume, and did assume, that Defendant had
3 secured their PII. At no time were Plaintiff and the Class on notice that their PII was not secure,
4 which Defendant had a duty to disclose.

5 170. Defendant also violated California Civil Code § 1798.150 by failing to implement
6 and maintain reasonable security procedures and practices, resulting in an unauthorized access and
7 exfiltration, theft, or disclosure of Plaintiff's and the Class's nonencrypted and nonredacted PII.

8 171. Had Defendant complied with these requirements, Plaintiff and the Class would not
9 have suffered the damages related to the data breach.

10 172. Defendant's conduct was unlawful, in that it violated the CCPA.

11 173. Defendant's acts, omissions, and misrepresentations as alleged herein were
12 unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

13 174. Defendant's conduct was also unfair, in that it violated a clear legislative policy in
14 favor of protecting consumers from data breaches.

15 175. Defendant's conduct is an unfair business practice under the UCL because it was
16 immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct
17 includes employing unreasonable and inadequate data security despite its business model of
18 actively collecting PII.

19 176. Defendant also engaged in unfair business practices under the "tethering test." Its
20 actions and omissions, as described above, violated fundamental public policies expressed by the
21 California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all
22 individuals have a right of privacy in information pertaining to them . . . The increasing use of
23 computers . . . has greatly magnified the potential risk to individual privacy that can occur from
24 the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the
25 Legislature to ensure that personal information about California residents is protected."); Cal. Bus.
26 & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online
27
28

Privacy Protection Act] is a matter of statewide concern.”). Defendant’s acts and omissions thus amount to a violation of the law.

177. Instead, Defendant made the PII of Plaintiff and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendant’s conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

178. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

179. For one, on information and belief, Plaintiff’s and the Class’s stolen PII has already been published—or will be published imminently—by cybercriminals on the dark web.

180. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

181. There were reasonably available alternatives to further Defendant’s legitimate business interests, other than the misconduct alleged in this complaint.

182. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant’s unlawful and unfair business activities; and any other equitable relief the Court deems proper.

SEVENTH CLAIM FOR RELIEF
Violations of the California Consumer Privacy Act (“CCPA”)
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff and the Class)

183. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

184. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiff and the Class. As a direct and proximate

1 result, Plaintiff's and the Class's nonencrypted and nonredacted PII was subject to unauthorized
2 access and exfiltration, theft, or disclosure.

3 185. Defendant is a "business" under the meaning of Civil Code § 1798.140 because
4 Defendant is a "corporation, association, or other legal entity that is organized or operated for the
5 profit or financial benefit of its shareholders or other owners" that "collects consumers' personal
6 information" and is active "in the State of California" and "had annual gross revenues in excess of
7 twenty-five million dollars (\$25,000,000) in the preceding calendar year." Civil Code §
8 1798.140(d).

9 186. Plaintiff and Class Members seek injunctive or other equitable relief to ensure
10 Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures
11 and practices. Such relief is particularly important because Defendant continues to hold PII,
12 including Plaintiff's and Class members' PII. Plaintiff and Class members have an interest in
13 ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing
14 to adequately safeguard this information.

15 187. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice
16 letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that
17 Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and
18 Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff
19 intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

20 188. As described herein, an actual controversy has arisen and now exists as to whether
21 Defendant implemented and maintained reasonable security procedures and practices appropriate
22 to the nature of the information so as to protect the personal information under the CCPA.

23 189. A judicial determination of this issue is necessary and appropriate at this time under
24 the circumstances to prevent further data breaches by Defendant.

25 **PRAYER FOR RELIEF**

26 Plaintiff and members of the Class demand a jury trial on all claims so triable and request
27 that the Court enter an order:

- 1 A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class,
2 appointing Plaintiff as class representative, and appointing his counsel to represent
3 the Class;
- 4 B. Awarding declaratory and other equitable relief as is necessary to protect the
5 interests of Plaintiff and the Class;
- 6 C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and
7 the Class;
- 8 D. Enjoining Defendant from further deceptive practices and making untrue
9 statements about the Data Breach and the stolen PII;
- 10 E. Awarding Plaintiff and the Class damages that include applicable compensatory,
11 exemplary, punitive damages, and statutory damages, as allowed by law;
- 12 F. Awarding restitution and damages to Plaintiff and the Class in an amount to be
13 determined at trial;
- 14 G. Awarding attorneys' fees and costs, as allowed by law;
- 15 H. Awarding prejudgment and post-judgment interest, as provided by law;
- 16 I. Granting Plaintiff and the Class leave to amend this complaint to conform to the
17 evidence produced at trial; and
- 18 J. Granting such other or further relief as may be appropriate under the
19 circumstances.

20 **JURY DEMAND**

21 Plaintiff hereby demands that this matter be tried before a jury.

22
23 Dated: May 2, 2024

Respectfully Submitted,

24 By: /s/ Andrew G. Gunem

25 Andrew G. Gunem (SBN 354042)
26 agunem@straussborrelli.com
27 STRAUSS BORRELLI PLLC
28 One Magnificent Mile
980 N Michigan Avenue, Suite 1610

Chicago IL, 60611

Attorneys for Plaintiff and Proposed Class